(/../)

Liferay 6.2

What is Liferay? (https://dev.liferay.com/discover/portal/-/knowledge_base/6-2/what-is-liferay)

Web Content Management (https://dev.liferay.com/discover/portal/-/knowledge_base/6-2/web-content-management)

Advanced Web Content Management (https://dev.liferay.com/discover/portal/-/knowledge_base/6-2/advanced-web-content-management)

Configuring Liferay Applications (https://dev.liferay.com/discover/portal/-/knowledge_base/6-2/configuring-liferay-applications)

Document Management (https://dev.liferay.com/discover/portal/-/knowledge_base/6-2/document-management)

Displaying Content Dynamically (https://dev.liferay.com/discover/portal/-/knowledge_base/6-2/displaying-

Edit on GitHub (https://github.com/liferay/liferay-docs/blob/6.2.x/discover/portal/articles/16-user-management/03-roles-and-permissions.markdown) (https://dev.liferay.com/discover/portal/-/knowledge_base/6-2/roles-and-permissions?p_p_lifecycle=2&p_p_resource_id=kbArticleRSS&p_p_cacheability=cacheLevelFull&_2_WAR_knowledgebaseportlet_resourcePrimKey=454645&_2_WAR_knowledgebaseportlet_resourceClassNameId=10441)

ROLES AND PERMISSIONS

Roles are used to collect permissions that define a particular function within the portal, according to a particular scope. Roles can be granted permissions to various functions within portlet applications. A roles is basically just a collection of permissions that defines a function, such as Message Board Administrator. A role with that name is likely to have permissions relevant to the specific Message Board portlets delegated to it. Users who are placed in this role will inherit these permissions.

If you navigate to the Control Panel and click on *Roles*, you'll find a single interface which lets you create roles, assign permissions to them, and assign users to the roles. Roles can be scoped by portal, site, or organization. To create a role, click the *Roles* link and then click the *Add* button. You can choose a Regular, Site or Organization role. A regular role is a portal-scoped role. Make a selection and then type a name for your role, a title and a description. The name field is required but the title and description are optional. If you enter a name and a title, the title will be displayed in the list of roles on the Roles page of the Control Panel. If you do not enter a title, the name will be displayed. When you have finished, click *Save*.

In addition to regular roles, site roles, and organization roles, there are also teams. Teams can be created by site administrators within a specific site. The permissions granted to a team are defined and applied only within the team's site. The permissions defined by regular, site, and organization roles, by contrast, are defined at the portal level, although they are applied to different scopes. The differences between the four types of roles can be described as follows:

- Regular role: Permissions are defined at the *portal* level and are applied at the *portal* level.
- Site role: Permissions are defined at the *portal* level and are applied to one *specific site*.
- Organization role: Permissions are defined at the *portal* level and are applied to one *specific organization*.
- Team: Permissions are defined within a *specific site* and are assigned within that *specific site*.

content-dynamically)

Targeting Content To Your Audience (https://dev.liferay.com/discover/portal/-/knowledge_base/6-2/targeting-content-to-your-audience)

Personalization and Customization (https://dev.liferay.com/discover/portal/-/knowledge_base/6-2/personalization-and-customization)

Collaboration Suite (https://dev.liferay.com/discover/portal/-/knowledge_base/6-2/collaboration-suite)

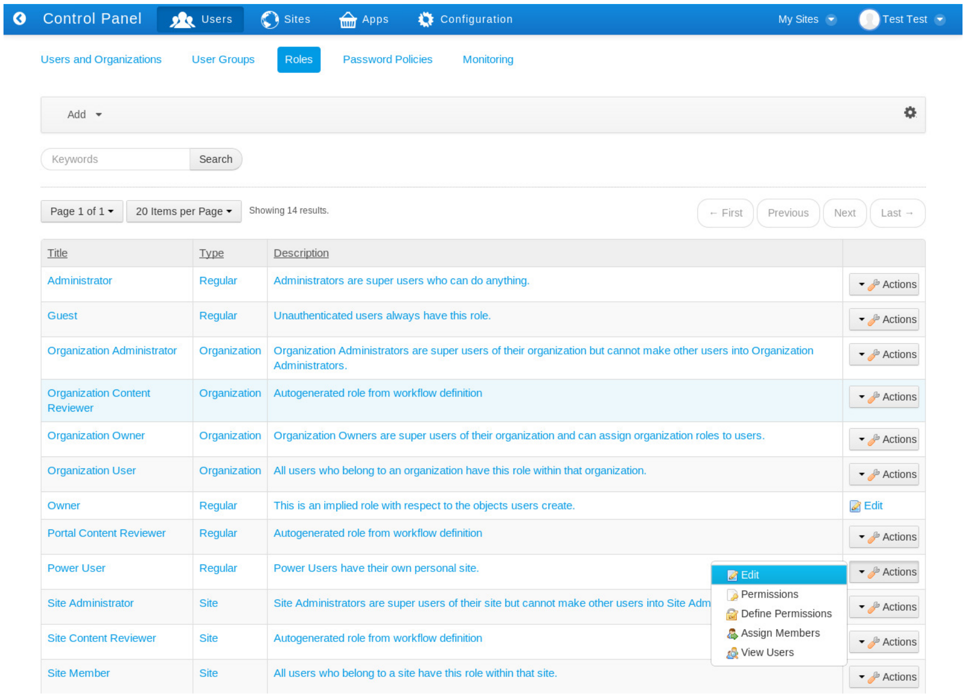
Social Networking (https://dev.liferay.com/discover/portal/-/knowledge_base/6-2/social-networking)

Using Web Forms and Dynamic Data Lists (https://dev.liferay.com/discover/portal/-/knowledge_base/6-2/using-web-forms-and-dynamic-data-lists)

Using Workflow (https://dev.liferay.com/discover/portal/-/knowledge_base/6-2/using-workflow)

Kaleo Forms: Defining Business Processes (https://dev.liferay.com/discover/portal/-/knowledge_base/6-2/kaleo-forms-defining-business-

Read here (/discover/portal/-/knowledge_base/6-2/creating-teams-for-advanced-site-membership-management)For more information about teams.



Title	Type	Description	
Administrator	Regular	Administrators are super users who can do anything.	Actions
Guest	Regular	Unauthenticated users always have this role.	Actions
Organization Administrator	Organization	Organization Administrators are super users of their organization but cannot make other users into Organization Administrators.	Actions
Organization Content Reviewer	Organization	Autogenerated role from workflow definition	Actions
Organization Owner	Organization	Organization Owners are super users of their organization and can assign organization roles to users.	Actions
Organization User	Organization	All users who belong to an organization have this role within that organization.	Actions
Owner	Regular	This is an implied role with respect to the objects users create.	Edit
Portal Content Reviewer	Regular	Autogenerated role from workflow definition	Actions
Power User	Regular	Power Users have their own personal site.	Actions
Site Administrator	Site	Site Administrators are super users of their site but cannot make other users into Site Adm	Actions
Site Content Reviewer	Site	Autogenerated role from workflow definition	Actions
Site Member	Site	All users who belong to a site have this role within that site.	Actions

Figure 16.9: To examine all the roles defined for your portal, navigate to the Control Panel and click on *Roles*.

After you save, Liferay redirects you to the list of roles. To see what functions you can perform on your new role, click the *Actions* button.

Edit: lets you change the name, title or description of the role.

Permissions: allows you to define which users, user groups or roles have permissions to edit the role.

Define Permissions: defines what permissions this role grants. This is outlined in the next section.

Assign Members: lets you search and select users in the portal to be assigned to this role. These users will inherit any permissions that have been assigned to this role.

View Users: allows you to view the users who have been assigned to this role.

Delete: permanently removes a role from the portal.

Next, let's learn about the difference between the (portal/site/organization) administrator and owner roles that Liferay provides out-of-the-box.

OUT-OF-THE-BOX LIFERAY ROLES

If you navigate to the Control Panel and click on *Roles*, you'll see a list of all the roles that have been created in your portal. This list includes roles that Liferay provides out-of-the-box and any additional custom roles. These are some of Liferay's out-of-the-box roles:

- Guest: The Guest role is assigned to unauthenticated users and grants the lowest-level permissions within the portal.
- User: The User role is assigned to authenticated users and grants basic basic permissions within the portal.
- Power User: By default, the Power User role grants the same permissions as the User role. It’s designed to be an extension point for distinguishing regular users from more privileged users. For example, you can set up your portal so that only Power Users have personal sites.
- Site Member: The Site Member role grants basic privileges within a site, such as the ability to visit the site’s private pages.
- Site Administrator: The Site Administrator role grants the ability to manage *almost* all aspects of a site including site content, site memberships, and site settings. Site Administrators cannot delete the membership of or remove roles from other Site Administrators or Site Owners. They also *cannot* assign other users as Site Administrators or Site Owners.
- Site Owner: The Site Owner role is the same as the Site Administrator role except that it grants the ability to manage *all* aspects of a site, including the ability to delete the membership of or remove roles from Site Administrators or other Site Owners. They *can* assign other users as Site Administrators or Site Owners.
- Organization User: The Organization User role grants basic privileges within an organization. If the organization has an attached site, the Organization User role implicitly grants the Site member role within the attached site.
- Organization Administrator: The Organization Administrator role grants the ability to manage *almost* all aspects of an organization including the organization’s users and the organization’s site (if it exists). Organization Administrators cannot delete the membership of or remove roles from other Organization Administrators or Organization Owners. They also *cannot* assign other users as Organization Administrators or Organization Owners.
- Organization Owner: The Organization Owner role is the same as the Organization Administrator role except that it grants the ability to manage *all* aspects of an organization, including the ability to delete the membership of or remove roles from Organization Administrators or other Organization Owners. They *can* assign other users as Organization Administrators or Organization Owners.
- Administrator: The administrator role grants the ability to manage the

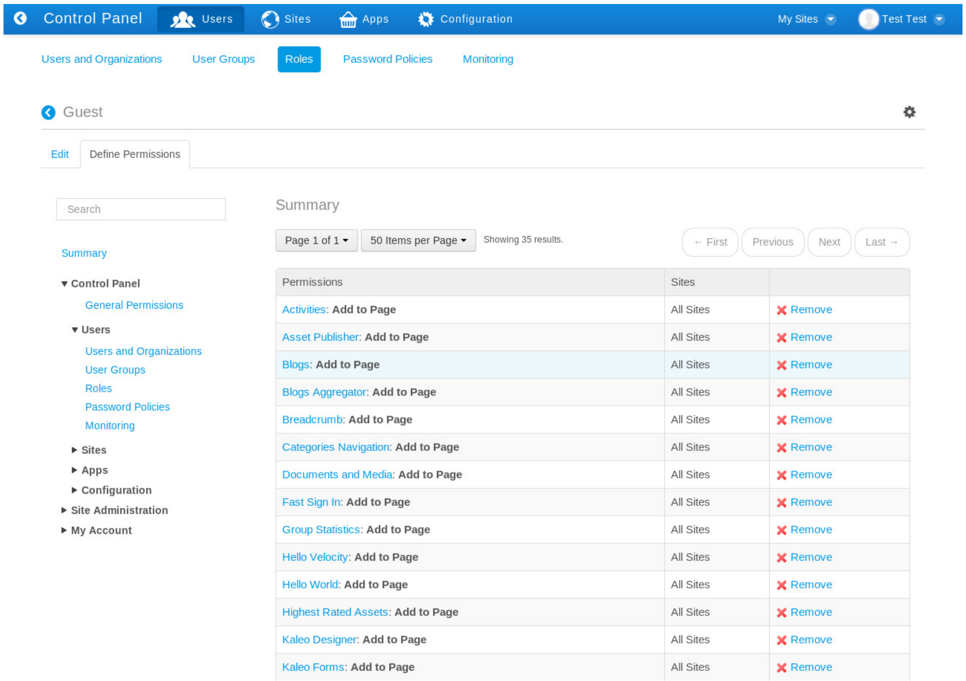
entire portal, including global portal settings and individual sites, organizations, and users.

> **Tip:** It's easy to overlook the differences between site and organization owners and site and organization administrators. Remember that site and organization administrators *cannot* delete the membership of or remove the administrator or owner role from any other administrator or owner. They also *cannot* appoint other users as site or organization administrators or owners. Site and organization owners *can* delete the membership of or remove the administrator or owner roles from other site or organization administrators. They *can* appoint other users as site or organization administrators or owners.

Next, let's examine how to configure the permissions granted by different roles.

DEFINING PERMISSIONS ON A ROLE

Roles serve as repositories of permissions. When a roles is assigned to a user, the user receives all the permissions defined by the role. So, to use a role, you need to assign members to it and define the permissions you want to grant to members of the role.



Summary

Showing 35 results.

Permissions	Sites	
Activities: **Add to Page**	All Sites	✖ Remove
Asset Publisher: **Add to Page**	All Sites	✖ Remove
Blogs: **Add to Page**	All Sites	✖ Remove
Blogs Aggregator: **Add to Page**	All Sites	✖ Remove
Breadcrumb: **Add to Page**	All Sites	✖ Remove
Categories Navigation: **Add to Page**	All Sites	✖ Remove
Documents and Media: **Add to Page**	All Sites	✖ Remove
Fast Sign In: **Add to Page**	All Sites	✖ Remove
Group Statistics: **Add to Page**	All Sites	✖ Remove
Hello Velocity: **Add to Page**	All Sites	✖ Remove
Hello World: **Add to Page**	All Sites	✖ Remove
Highest Rated Assets: **Add to Page**	All Sites	✖ Remove
Kaleo Designer: **Add to Page**	All Sites	✖ Remove
Kaleo Forms: **Add to Page**	All Sites	✖ Remove

Figure 16.10: When defining permissions on a role, the Summary view provides a list of permissions that have already been defined for the role. The area on the left side of the screen lets you drill down through various categories of portal permissions.

When you click on the *Actions* button for a portal-scoped role and select *Define Permissions*, you'll see a list of all the permissions that have been defined for that role. To add permissions to a role, drill down through the categories of permissions on the left side of the screen and click on a specific category (such as *Site Administration → Pages → Site Pages*. In the center of the screen, you'll see the permissions that belong to that category. Flag the checkboxes next to the permissions that you'd like to add the role, then click *Save*. For non-portal scoped roles, you need to click on the *Options* link on individual portlets, then *Configuration*, then *Permissions* to assign permissions within the site that owns the portlet.

Portal permissions cover portal-wide activities that comprise several categories, such as site, organization, location, password policy, etc. This allows you to create a role that, for example, can create new sites within the portal. This would allow you to grant users that particular permission without making them overall portal administrators.

For Liferay 6.2, the permissions fall into the following hierarchy of categories:

- Control Panel
  - General Permissions
  - Users
    - Users and Organizations
    - User Groups
    - Roles
    - Password Policies
    - Monitoring
  - Sites
    - Sites
    - Site Templates
    - Page Templates
  - Apps
    - Store
    - Purchased
    - App Manager
    - Plugins Configuration
    - License Manager
  - Configuration
    - Portal Settings
    - Custom Fields
    - Server Administration
    - Portal Instances
- Site Administration
  - Pages
    - Site Pages
  - Content
    - Recent Content

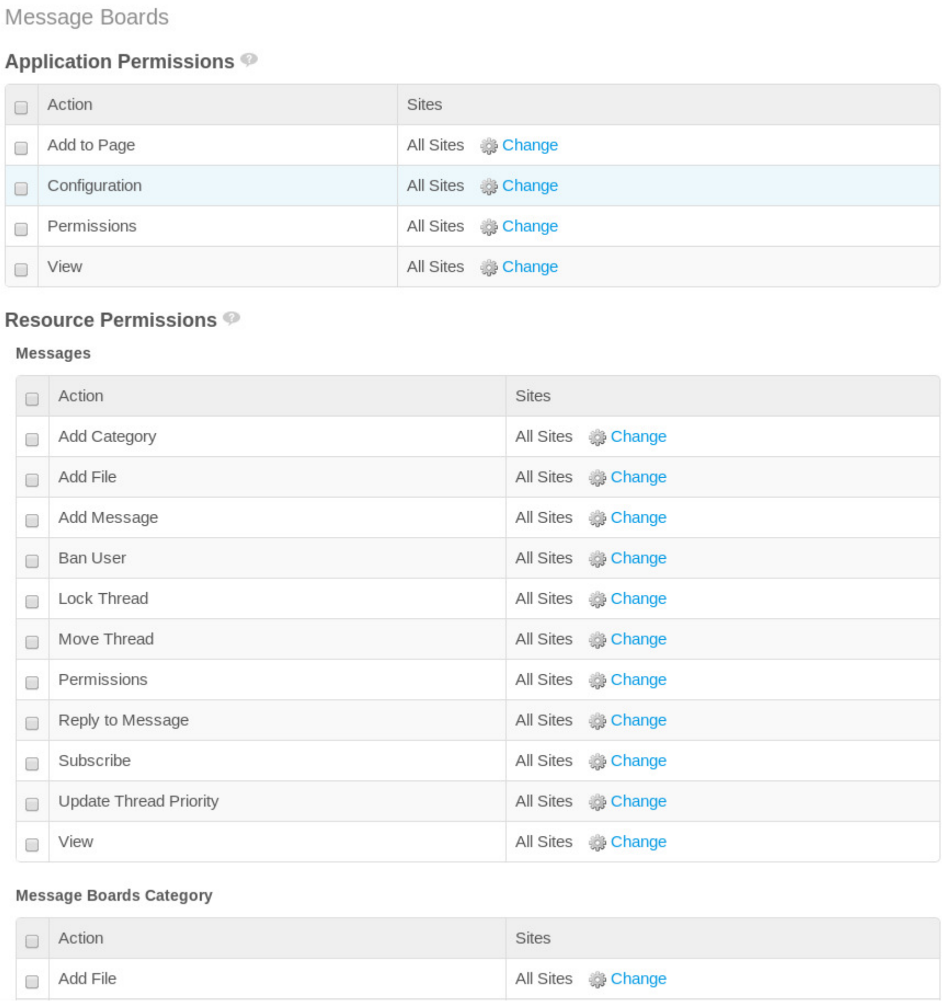
    - Web Content
    - Documents and Media
    - Blogs
    - Message Boards
    - Wiki
    - Dynamic Data Lists
    - Bookmarks
    - Polls
    - Software Catalog
    - Tags
    - Categories
    - Recycle Bin
  - Users
    - Site Memberships
    - Site Teams
  - Configuration
    - Site Settings
    - Site Template Settings
    - Application Display Templates
    - Social Activity
    - Mobile Device Families
  - Applications
    - [too many to list]
- My Account
  - Account Settings
  - My Pages

The three basic categories of permissions are Control Panel, Site Administration, and My Account. By default, any portal user can manage their user account via the permissions belonging to the My Account category. Site administrators can access the site administration tools belonging to the Site Administration category. And portal administrators can access the entire Control Panel. For custom roles, you can mix and match permissions from as many categories as you like.

The permissions in the Site Administration → Applications categories govern the content that can be created by core portlets such as the Wiki and Message Boards. If you pick one of the portlets from this list, you'll get options for defining permissions on its content. For example, if you pick Message Boards, you'll see permissions for creating categories and threads or deleting and moving topics.

Site application permissions affect the application as a whole. So, using the Message Boards as an example, an application permission might define who can add the Message Boards portlet to a page.

The Control Panel permissions affect how the Control Panel appears to the user in the Control Panel. The Control Panel appears differently to different users, depending on their permissions. Some Control Panel portlets have a Configuration button and you can define who gets to see that. You can also fine-tune who gets to see various applications in the Control Panel.



Message Boards

Application Permissions

□	Action	Sites
□	Add to Page	All Sites Change
□	Configuration	All Sites Change
□	Permissions	All Sites Change
□	View	All Sites Change

Resource Permissions

Messages

□	Action	Sites
□	Add Category	All Sites Change
□	Add File	All Sites Change
□	Add Message	All Sites Change
□	Ban User	All Sites Change
□	Lock Thread	All Sites Change
□	Move Thread	All Sites Change
□	Permissions	All Sites Change
□	Reply to Message	All Sites Change
□	Subscribe	All Sites Change
□	Update Thread Priority	All Sites Change
□	View	All Sites Change

Message Boards Category

□	Action	Sites
□	Add File	All Sites Change

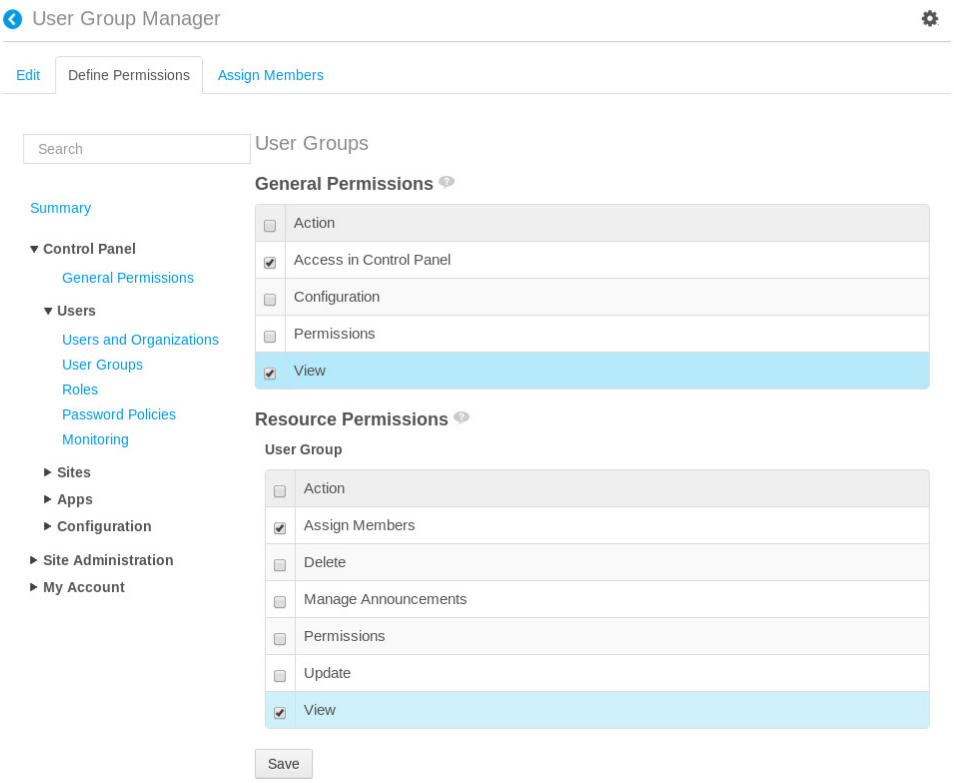
Figure 16.11: You can fine-tune which actions are defined for a role within a specific application like the Message Boards.

Each possible action to which permissions can be granted is listed. To grant a permission, flag the checkbox next to it. If you want to change the scope of a permission, click the *Change* link next to the gear icon next to the permission and then choose a new scope. After you finish defining permissions for a role, click *Save*. For a portal-scoped Message Boards Administrator role, you might want to grant content permissions for every Message Boards action listed. After you click *Save*, you'll see a list of all permissions currently granted to the role. From the Summary view, you can add more permissions or go back by clicking on the *Back* icon.

The list of permissions that you can define for a role may seem overwhelming. However, these permissions ensure that you can customize exactly which areas of your portal you'd like different collections of users to be able to access. Sometimes you might find that a certain permission grants more or less access than what you expected–always test your permissions configurations!

For example, suppose that you need to create a role called User Group Manager. You'd like to define the permissions for the User Group Manager role so that users assigned to this role can add users to or remove users from any user group. To do this, you can take the following steps:

1. Click on *Admin* → *Control Panel* from the Dockbar and then click on *Roles*.
2. On the Roles screen, click *Add* → *Regular Role*.
3. After naming your role and entering a title, click *Save*.
4. Click on *Define Permissions* and drill down in the menu on the left to *Control Panel* → *Users* → *Users and Organizations*.
5. Under the *General Permissions* heading, flag *Access in Control Panel* and *View*. This lets user group managers access the User Groups Control Panel portlet and view existing user groups.
6. Since you'd like user group managers to be able to view user groups and assign members to them, you'd also check the *Assign Members* and *View* permissions under the *Resource Permissions* → *User Group* heading.
7. Click *Save*.



User Groups

General Permissions

□	Action
☑	Access in Control Panel
□	Configuration
□	Permissions
☑	View

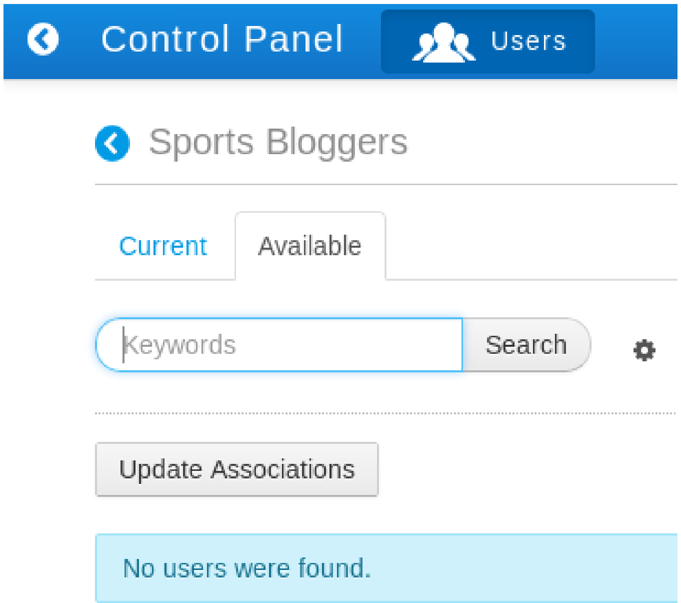
Resource Permissions

User Group

□	Action
☑	Assign Members
□	Delete
□	Manage Announcements
□	Permissions
□	Update
☑	View

Figure 16.12: Make sure to test the permissions you grant to custom roles.

You might expect that these permissions would be enough to allow users assigned to the User Group Manager role to add or remove any users to or from any user group. After all, we've granted user group managers permissions to view user groups and assign members and we've granted them access to User Groups in the Control Panel. However, we're forgetting an important permission. Can you guess what it is? That's right: we haven't granted the User Group Manager role permission to view users! Although user group managers can assign members to user groups, they don't have permission to view users at the portal level. This means that if they click *Assign Members* for a user group and click on the *Available* tab, they'll see an empty list.



No users were found.

Figure 16.13: Users assigned to the User Group Manager role can't find any users to add!

To fix this, log in as an administrator and click *Admin* → *Control Panel* from the Dockbar. Then click on *Roles* and then on *Actions* → *Define Permissions* next to the *User Group Manager* role. Then, drill down to the *Control Panel* → *Users* → *Users and Organizations* category and flag the *View* permission under the *Resource Permissions* → *User* heading. *View*. Click *Save*. Once you've saved your permissions configuration, users who've been assigned to the User Group Manager role will be able to browse the portal's entire list of users when assigning users to a user group.

Roles are very powerful and allow portal administrators to define various permissions in whatever combinations they like. This gives you as much flexibility as possible to build the site you have designed.

PERMISSION FOR DELEGATING SOCIAL ACTIVITIES CONFIGURATION

As of Liferay 6.2, there's a permission that allows site administrators to delegate responsibility for configuring social activities to other users. To assign this permission to a role, first navigate to the Control Panel and click on *Roles*. If you'd like to add a new role, do so. Then click *Actions* next to the role to which you'd like to add social activities configuration permissions and select *Define Permissions*. Next, drill down to the *Site Administration* →

Configuration → *Social Activity* permissions category. Flag all of the permissions and then click *Save*:

- Access in Site Administration
- Configuration
- Permissions
- View

Once these permissions have been assigned to the chosen role, any users assigned to the role will be able to manage your site's Social Activities configuration.

NOTE ABOUT PERMISSIONS FOR DELETING CONTAINERS

Liferay Portal contains many types of portal resources upon which permissions can be defined. These include both assets and asset containers. The term *asset* refers to any kind of content in Liferay such as a web content article, blog entry, wiki article, message board post, or Documents and Media document. Asset containers are portal resources used for grouping specific kinds of assets. For example, web content folders, wiki nodes, message board categories, and Documents and Media folders are asset containers.

When configuring permissions for assets and asset containers, it's important to note that the permission to delete an asset container includes the permission to indirectly delete any assets in the container. This means that if a user has permission to delete an asset container, the user can delete all of the assets in that container even the user lacks permission to delete any of the assets in the container individually. Granting permission to delete a folder but not any of the contained assets is *not* a common use case. Nevertheless, it's important to note that assets in a container can be indirectly deleted if their asset container is deleted.

NOTE ABOUT THE POWER USERS ROLE

Prior to Liferay 6.0, the default configurations of many Liferay portlets allowed power users, but not regular users, to access them. Liferay 6.0 and subsequent versions grant the same default permissions to both power users and regular users. This way, portal administrators are not forced to use the power users role. However, Liferay encourages those who do to create their own custom permissions for the role.

> **Note:** Prior to Liferay version 6.0, Power Users and Users did *not* have the same default permissions. So if are using Liferay 5.2 or a previous version, it's dangerous to remove the Power Users role from the default user associations: this could remove certain permissions you expect to apply to all users. If you decide to remove the Power Users

> role from the default user associations anyway, you will probably want to modify the permissions on certain portlets to make them accessible to all users. To do this, see the section on Plugins Configuration below.

Now that we've seen how to use organizations and user groups to manage users and how to use roles to define permissions, let's learn how to configure portal password policies.

PASSWORD POLICIES

Password policies can enhance the security of your portal. You can set requirements on password strength, frequency of password expiration, user lockout, and more. Additionally, you can apply different password policies to different sets of portal users. You define custom password policies or delegate user authentication to an LDAP server.

If you are viewing a page other than the Control Panel, click on *Admin* → *Control Panel* from the Dockbar. Next, click on the *Password Policies* link under the *Users* heading. You'll see that there's already a default password policy in the system. You can edit this in the same manner as you edit other resources in the portal: click *Actions* and then click *Edit*.

The Password Policy settings form contains the following fields. Enabling specific settings via the check boxes prompts setting-specific options to appear.

Name: requires you to enter a name for the password policy.

Description: lets you describe the password policy so other administrators will know what it's for.

Changeable: determines whether or not a user can change his or her password.

Change Required: determines whether or not a user must change his or her password after logging into the portal for the first time.

Minimum Age: lets you choose how long a password must remain in effect before it can be changed.

Reset Ticket Max Age: determines how long a password reset link remains valid.

Password Syntax Checking: allows you to set a minimum password length and to choose whether or not dictionary words can be in passwords. You can also specify detailed requirements such as minimum numbers of alpha numeric characters, lower case letters, upper case letters, numbers or symbols.

Password History: lets you keep a history (with a defined length) of passwords and prevents users from changing their passwords to one that was previously used.

Password Expiration: lets you choose how long passwords can remain active before they expire. You can select the age, the warning time and a grace limit.

Lockout: allows you to set a number of failed log-in attempts that triggers a user's account to lock. You can choose whether an administrator needs to unlock the account or if it becomes unlocked after a specific duration.

From the list of password policies, you can perform several other actions.

Edit: brings you to the form above and allows you to modify the password policy.

Permissions: allows you to define which users, user groups or roles have permission to edit the password policy.

Assign Members: takes you to a screen where you can search and select users in the portal to be assigned to this password policy. The password policy will be enforced for any users who are added here.

Delete: shows up for any password policies you add beyond the default policy. You cannot delete the default policy.

+1 (1 Vote)

User Groups (https://dev.liferay.com/discover/portal/-/knowledge_base/6-2/user-groups)

Monitoring (https://dev.liferay.com/discover/portal/-/knowledge_base/6-2/monitoring)